## AD NUMBER

**ADB257113**

## NEW LIMITATION CHANGE

TO

**Approved for public release, distribution unlimited**

FROM

**Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use 19 Jun 2000 Other requests shall be referred to DTIC-AI, Fort Belvoir, VA 22060-6218**

## AUTHORITY

**IATAC ltr, 21 Aug 2001**

# White House Document

9/13/99

ANALYSIS

THE CYBERSPACE ELECTRONIC SECURITY ACT OF 1999

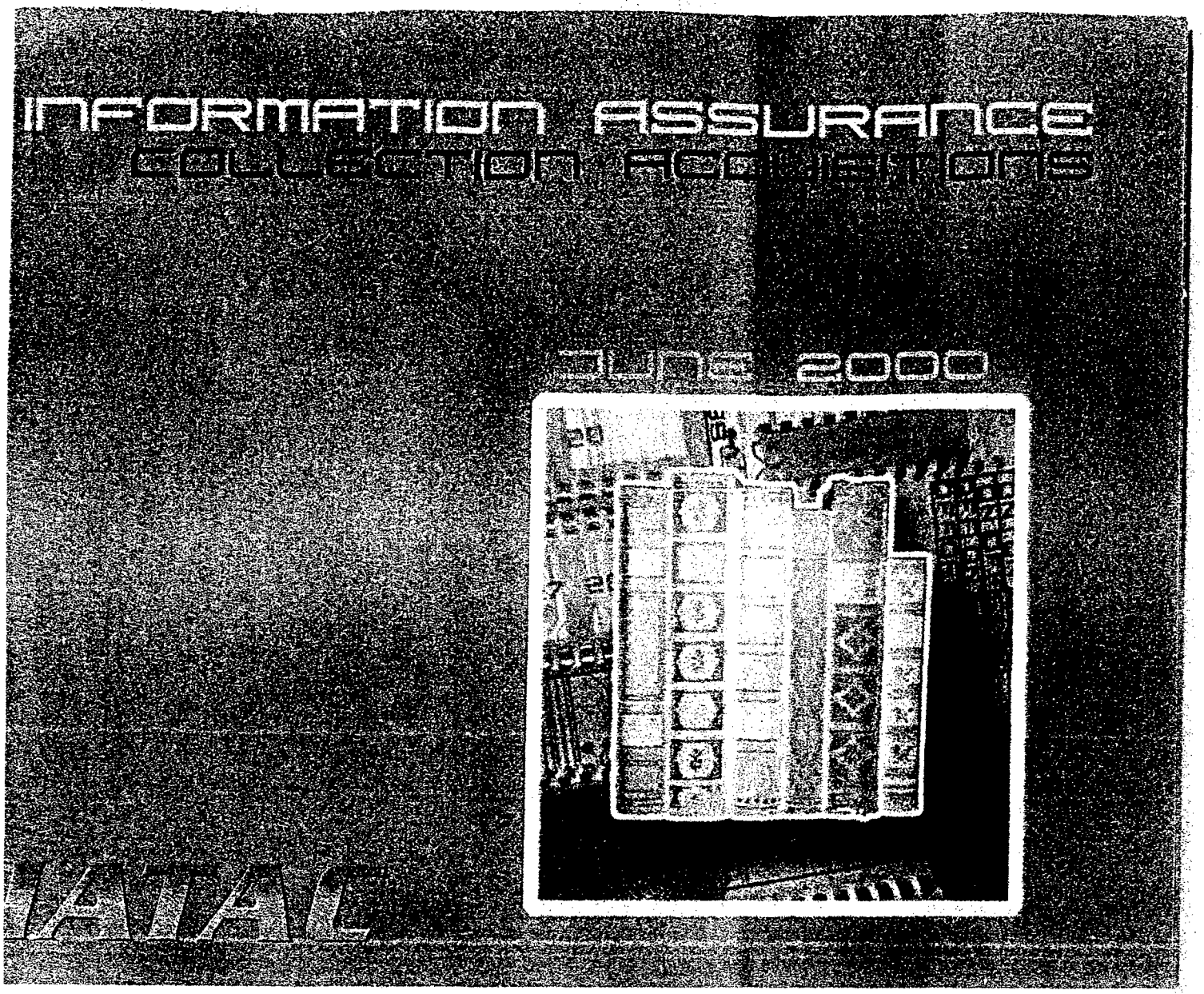
The Cyberspace Electronic Security Act of 1999 (CESA) updates law enforcement and privacy rules for our emerging world of widespread cryptography, which is a tool to protect the confidentiality of wire and electronic communications and stored data. Cryptography has many legitimate and important uses. It also is increasingly used as a means to facilitate criminal activity, such as drug trafficking, terrorism, white collar crime, and the distribution of child pornography. The Act responds to both the legitimate and unlawful uses of cryptography, building a legal infrastructure for these emerging issues.

CESA recognizes that the use of cryptography for legitimate purposes should be protected. Currently there are no federal statutory protections for the privacy of decryption keys per se. CESA would create such protections, limiting in many cases the disclosure of decryption keys to both public and private entities. In particular, CESA recognizes the role of "recovery agents" in today's information age. Recovery agents provide storage services for keys that can be used to decrypt data and communications. Such storage services play an important role in protecting encrypted data because of the possibility, for example, that a person who encrypts data will lose the decryption key and later need it to decrypt the data, or that such person's heirs will require a decryption key for legitimate purposes. When a person stores a decryption key or other recovery information with a recovery agent, the Act creates new protections. It prohibits the recovery agent from disclosing such information or using it to decrypt data except under limited circumstances, such as with the consent of the person who stored the key or under a court order. The Act also promotes privacy and security by prohibiting a recovery agent from selling or otherwise disclosing its customer lists to other parties.

While decryption keys must be protected from improper disclosure, CESA recognizes the need for government access to keys for legitimate law enforcement purposes. The Act, therefore, authorizes a recovery agent to disclose stored recovery information to the government, or to use stored recovery information on behalf of the government, in a narrow range of circumstances, for example, pursuant to a search warrant or in accordance with a court order under the Act. Such a court order must be based on a finding that, among other things, there is no constitutionally protected expectation of privacy in the plaintext of encrypted data or that the privacy interest created by such expectation has been overcome by consent, warrant, order, or other authority. Thus, CESA reflects a careful balancing of the interests of public safety and privacy. Currently, in the absence of statutory protections for the privacy of stored recovery information, the government may be able to obtain stored recovery information from a recovery agent with, for example, a grand jury subpoena. CESA makes clear that the government may not seek stored recovery information from a recovery agent through such a mechanism, standing alone.

CESA also recognizes that law enforcement personnel may need the plaintext of encrypted data when a decryption key for the data is not held by, or is not obtained from, a recovery agent. In the pre-encryption world, this problem did not arise. Today, when law enforcement personnel obtain written materials, they can normally read them. In the future, as encryption becomes more widespread, "written" materials may often not be readable without a decryption key, and, when the key is not stored with a recovery agent, the government will need another way to obtain decryption keys or plaintext. The government, using existing legal authorities, will have to attempt to use techniques to obtain usable evidence in such cases; however, those techniques are likely to be of little use if they are revealed because informing criminals about government investigative methods will provide a road map showing how to avoid authorized law enforcement activity. Therefore, in order to permit the continued use of such techniques, CESA provides for the issuance of court orders to protect the confidentiality of such techniques under specified circumstances (such as upon a finding that disclosure is likely to compromise a technique for purposes of future investigations or to result in injury to any person) and requires such orders to be consistent with constitutional principles.

While CESA reflects the need for law enforcement access to recovery information, it also provides limitations on the use and disclosure or such information obtained through compulsory process. For example, CESA requires that a court order




e-mail: iatac@dtic.mil URL: http://iac.dtic.mil/iatac SIPRNET: http://iac.dtic.smil.mil
3190 Fairview Park Drive, Falls Church, VA 22042

authorizing government access to stored recovery information specify the categories of data and communications that may be decrypted using the recovery information. In addition, CESA requires the eventual destruction of recovery information obtained through compulsory process. The limitations on the use and disclosure of recovery information obtained through compulsory process and the requirement for the destruction of such information reflect CESA's balancing of the need for privacy against the need for law enforcement access in appropriate circumstances to such information.

Section 201

Section201 of CESA redesignates the definitional provision of chapter121 of title18, United States Code, which concerns stored wire and electronic communications and transactional records access. Currently, the definitional provision is in section2711 but would be expanded and redesignated as section2718 by CESA.

Section 202

Section202 amends sections2703(d) of title18, UnitedStates Code, which concerns government access to the contents of electronic communications held by an electronic communications service or a remote computing service and to subscriber information and related records held by such entities. Currently, under section 2703(d) a court order for disclosure may be issued by a federal district court (including a magistrate of such court) or a federal court of appeals. Under the amendment such an order could be issued by any "court of competent jurisdiction." Section2718 defines this term to include both a court of general criminal jurisdiction of a State authorized by State law to enter orders authorizing the use of a pen register or trap and trace device and also a federal court in the categories specified under current law, without geographic limitation. Thus, the amendment provides that a State court can issue an order under section 2703(d), and it clarifies that any federal court may issue an order under that section, not just a federal court in the district of the entity served with the order.

Section 202 of CESA also amends section 2707 of title 18, United States Code, concerning civil actions for persons aggrieved by a violation of chapter121 of that title. First, this amendment makes a conforming change to recognize the exception to civil liability provided in proposed section2715, discussed below. It also amends subsection (e) of section2707 to add two new bases for a defense to civil or criminal liability. The first is a good faith reliance on a request of a governmental entity under section2703(f) for a provider of wire or electronic communication services or a remote computing service to preserve records and other evidence in its possession pending the issuance of a court order or other process. The second is a good faith reliance on an emergency request under proposed section 2712(a)(4) for the disclosure to a governmental entity by a recovery agent of stored recovery information or the use of it to decrypt data or communications (discussed below in the analysis of proposed section 2712). This amendment is parallel to the existing defense in section 2707(e) based on a good faith reliance on an emergency request under the wiretap statute, 18 U.S.C. § 2518(7). While requests under section 2703(f) or proposed section 2712(a)(4) are already included in the good faith defense because each provides a "statutory authorization" under section 2707(e)(1), this amendment makes the existence of such defense clear.

Section 203

Section203 adds a number of new provisions to chapter121 of title18, United States Code, to address decryption keys and other recovery information.

Proposed 18U.S.C. §2711

New section2711 in title18 addresses the disclosure or use of stored recovery information, such as decryption keys that can be used to decrypt data or communications, and notification of storage location. This proposed section prohibits a recovery agent from disclosing decryption keys and other stored recovery information, from using such information to decrypt data or communications, and from disclosing any other information or record that identifies a person or entity for whom the recovery agent holds or has held stored recovery information, except as specifically provided. Proposed section2711 also prohibits a person from knowingly obtaining stored recovery information from a recovery agent if the person knows or has reason to

know he or she has no lawful authority to do so. In addition, this section requires a recovery agent to inform any person who stores recovery information with that agent of the location or locations where the recovery information is stored--i.e., the country and/or state in which the recovery information is stored, but not the actual physical address.

The confidentiality of decryption keys stored with recovery agents is increasingly important as the use of encryption grows. The public must have confidence that storage is safe, much the same as the public must have confidence in the protection provided to papers stored in a safe deposit box at a bank. However, in limited circumstances third parties must be able to obtain access to decryption keys. Thus, proposed section2711(b)(1)(A)(ii) authorizes the disclosure or use of stored recovery information by a recovery agent in the case of a person who is determined by a court to be legally entitled under generally applicable law to receive, possess, or use stored recovery information (e.g., an heir who is determined by a court to be legally entitled to obtain a decedent's stored recovery information). In addition, a recovery agent may disclose or use stored recovery information with the consent of the person who stored the recovery information or that person's agent. Both of these permitted disclosures or uses apply when the disclosure is to, or use is on behalf of, any person or entity, including a governmental entity. Proposed section2711(b)(1)(B) also authorizes disclosure or use in the case of a governmental entity pursuant to a search warrant or other means set forth in proposed section 2712, discussed below.

It is important to note that a governmental entity need not seek access to recovery information under section 2712, but can also seek access based on the consent or "generally applicable law" provisions of section 2711(b)(1)(A). "Generally applicable law" is intended to include any law that generally covers ownership, control, or use of property or information, such as contract, agency, property, and estate laws, but does not include laws specifically addressing ownership, control, or use of recovery information only, or laws that support access to information in criminal investigations only. Therefore, the "generally applicable law" provision would not allow a State to pass a law lowering standards of access below those set by new section 2712.

It is also important to recognize that the definition of "recovery agent" in proposed section 2718 includes officers, employees and agents of the recovery agent. A disclosure to such persons is not prohibited by the Act, for example, as might occur incidentally in testing the security of the recovery agent's systems, because there is no disclosure to a person other than the recovery agent.

As noted above, section 2711, in order to protect privacy and to restrict the ability of criminals to target particular recovery agents, also limits the disclosure by a recovery agent of other information about those persons who store "stored recovery information" with the recovery agent. Section 2711(b)(2) allows a recovery agent to disclose information or a record, other than stored recovery information, that identifies a person or entity for whom the recovery agent holds or has held stored recovery information, only with consent, as is necessarily incident to the rendition of the service provided to that person or entity or to the protection of the rights or property of the recovery agent, in response to a court order based on compelling need and after notice to the person who stored the recovery information and an opportunity for him to be heard, or to the government in response to a warrant, a court order, or a subpoena. No notice is required to the subscriber when providing such information to the government, and any notice can be delayed upon a showing of good cause.

Proposed section 2711 includes a confidentiality provision in subsection (c) that prohibits a recovery agent from disclosing the fact that a governmental entity has required a recovery agent to disclose or use stored recovery information. It also prohibits a recovery agent from disclosing to any other person any decrypted data or communications provided to the governmental entity. Without such a prohibition investigations that utilize stored recovery information obtained by the government under CESA could be jeopardized when the person who stored a decryption key with a recovery agent learns of the disclosure to the government and re-encrypts using a new key or takes other action intended to thwart the government's efforts.

Proposed section 2711(d) provides exclusions. First, it clarifies that nothing in section2711 or 2712 prohibits a recovery agent from using or disclosing plaintext in its possession, custody, or control (except as provided in subsection(c)). This is self-evident--CESA is not intended to affect the standards for government access to plaintext in the hands of a person receiving appropriate process. In this regard, it is also appropriate to note that CESA does not prohibit or limit the ability of a person to respond to an authorized demand for plaintext information if such person has custody or control of the plaintext information, but maintains that same information in encrypted form. Thus, if an entity (which could be a recovery agent, or not) encrypted its own records and stored the recovery information with a recovery agent, CESA would not restrict the ability of the government to subpoena those records in plaintext form from the first entity &endash; the one who owned the records &endash; because the government would only be demanding the production of plaintext information from the

custodian of that information. In other words, CESA does not require an enhanced legal showing for the government to obtain records from the owner of the records, even if that entity happens to be a recovery agent.

Section 2711(d) also clarifies that nothing in proposed section2711 or 2712 prohibits a recovery agent from using or disclosing recovery information that is not "stored recovery information" held by it under the circumstances described in the definition of this term in proposed section2718(7). The distinction between "recovery information" and "stored recovery information" is important. As provided in proposed section2718, the former is merely a key or other data or object that can be used to decrypt data or communications. Stored recovery information differs in two particulars. It must be: 1)held by a recovery agent on behalf of someone else, and 2)stored under a confidentiality arrangement.

Each of the above two elements must be present for recovery information to qualify for the enhanced protections of stored recovery information. This is so because no new restrictions are necessary regarding a person's disclosure or use of his or her own recovery information, including when the government seeks it from the user, since the Fourth and Fifth Amendments to the Constitution provide protections applicable to a person's own recovery information in his or her possession. Moreover, there is no constitutionally protected expectation of privacy in recovery information held by a third party but not under a confidentiality arrangement. For example, if a person gives his or her recovery information to another with no limitations on its use, then the former has no reasonable expectation that the recovery information will be protected from further disclosure. In addition, if a person stores plaintext with a third party, such as an electronic communications service, who on its own initiative encrypts the information to protect it, the person who stores the plaintext has no enhanced expectation of privacy unless the electronic communications service agrees that it will decrypt the information only as instructed by the person who stored the plaintext. For these reasons, "stored recovery information," as defined in proposed section2718, requires confidentiality. It remains the exclusive property of the person who arranged for its storage with a recovery agent and, except as provided by CESA, may be disclosed or used by the recovery agent only with the consent of that person or that person's agent.

It should be noted that while the distinction between "recovery information" and "stored recovery information" is important with respect to the prohibition against disclosure or use by recovery agents, including disclosure to government entities, other aspects of CESA do not make such a distinction and protect "recovery information" that is not "stored recovery information" in other ways. For example, CESA includes notification requirements for both recovery information and stored recovery information when obtained by a governmental entity by compulsory process from a third party who holds it on behalf of another, as explained below. (See discussion of proposed sections 2712(c) and 2714.)

Proposed section2711(d)(3) specifically addresses "stored recovery information" and clarifies another exception to prohibited disclosure. It states that nothing in section2711 or 2712 prohibits a recovery agent from using stored recovery information to decrypt data or communications if applicable statutes, regulations, or other legal authorities otherwise require the recovery agent to provide such data or communications to a governmental entity in plaintext or similar form. For example, CESA is not intended to limit any disclosure requirements of the Bank Secrecy Act and other laws that require institutions to disclose records to the government or to maintain records for government inspection. Proposed section2711(d)(3) is important in order to clarify that institutions required by law to disclose or maintain records for government inspection may not evade those obligations by encrypting the records.

Proposed section2711(e) would establish criminal penalties, with a one-year maximum prison term, for violations of the disclosure prohibitions of section2711.

Proposed 18U.S.C. § 2712

Section203 of CESA also creates a new section2712 in title18, United States Code, which sets forth special requirements for governmental access to stored recovery information. This section provides protections for persons who store recovery information with a recovery agent since the section limits the means of governmental access to such information. Existing means of government access to stored recovery information will no longer apply unless they are authorized. For example, a governmental entity will not be able in a criminal investigation to compel disclosure of stored recovery information from a recovery agent through a grand jury subpoena, unless disclosure is permitted by section2711(b)(1)(A)(i), which requires the consent of the person or entity who stored the recovery information.

It is important to note that new section 2712 reaches only the disclosure or use of "stored recovery information" (discussed above in connection with proposed section 2711(d)). Just as CESA does not prohibit the use or disclosure either of

recovery information that is not "stored recovery information" or of plaintext that is in the recovery agent's possession, custody, or control, CESA does not present any obstacles to a governmental entity's obtaining such information. Further, section2712 does not restrict the government's access to recovery information held by someone who is not a recovery agent, such as a neighbor or friend who holds another person's decryption key for safekeeping. A governmental entity may use existing means to obtain such plaintext or recovery information.

CESA recognizes that in certain circumstances the privacy interest of a person who has stored a decryption key with a recovery agent must give way to the public interest in effective law enforcement. Proposed section2712 allows a governmental entity to require a recovery agent to disclose stored recovery information or to decrypt data or communications using stored recovery information, but section2712 authorizes compelling such disclosure or decryption through four mechanisms only: (1)pursuant to a search warrant or wiretap order; (2) under federal or State process to compel disclosure that is permitted by section 2711(b)(1)(A)(i), which requires the consent of the person or entity who stored the recovery information; (3)in accordance with a court order under proposed section2712(b); or (4)pursuant to a determination by a qualifying law enforcement officer that a specified type of emergency situation exists.

The first and fourth mechanisms for governmental access to stored recovery information are set forth in proposed section2712(a)(1) and (4) and are straightforward. The first is through a warrant under the Federal Rules of Criminal Procedure or an equivalent State warrant or through a wiretap order under section2518 of title18, United States Code. The fourth mechanism, the emergency authority provision, is modeled after a similar provision of the wiretap statute, 18U.S.C.§2518(7), and a similar provision of the pen register/trap and trace statute, 18 U.S.C. §3125. The proposed provision recognizes that an emergency situation may arise in which there is insufficient time to obtain a court order for the disclosure of stored recovery information or decryption by a recovery agent, for example, where there is immediate danger of death or serious physical injury to any person. However, disclosure is carefully restricted: the emergency basis may be determined only by a law enforcement officer specifically listed in the proposed amendment, there must be grounds upon which a court order under section2712 could be entered, and such an order must be sought within 48hours after the stored recovery information has been released or decryption has occurred.

The second and third approaches for governmental access to stored recovery information or decryption of data or communications, as outlined in proposed section2712(a)(2) and (3), reflect a careful balancing of the interests of public safety and privacy. Currently there are no federal statutory protections for the privacy of stored recovery information perse. Thus, for example, a grand jury subpoena may provide a mechanism for law enforcement personnel to obtain such information from a recovery agent, without any independent basis for disclosure. CESA creates privacy protections in this regard that do not exist under current law. Under proposed section2712(a)(2) a grand jury or other subpoena only provides a mechanism for a governmental entity to require a recovery agent to disclose or use stored recovery information in the limited circumstances in which disclosure is permitted by section2711(b)(1)(A)(i), which requires the consent of the person or entity who stored the information, or such person's or entity's agent. In an unusual case a recovery agent may refuse to disclose stored recovery information to a governmental entity even though the person who stored the information has consented to disclosure. In such a case CESA authorizes the use of a subpoena or other process under federal or State law to compel disclosure of stored recovery information or the use of stored recovery information to decrypt data or communications. Thus, CESA strictly limits the use of subpoenas with respect to stored recovery information.

Not only does the restricted use of a subpoena under CESA reflect a careful balancing of privacy and public safety interests, so does the court-order approach to governmental access to stored recovery information set forth in proposed section2712(a)(3). It authorizes a governmental entity to require a recovery agent to disclose stored recovery information or to use stored recovery information to decrypt data or communications pursuant to a court order that meets the requirements of section2712(b). This provision sets forth four criteria for a court order: (1)the use of the stored recovery information is reasonably necessary to allow access to the plaintext of data or communications; (2)access is otherwise lawful; (3)the governmental entity will seek access within a reasonable time; and (4)there is no constitutionally protected expectation of privacy in the plaintext, or the privacy interest created by the expectation has been overcome by consent, warrant, order, or other authority. A court must issue an order under section2712(b) if it finds, based on "specific and articulable facts," that the above criteria are satisfied.

It is important to recognize that the key requested must, under section 2712(b)(1), be "reasonably necessary" to allow access to the plaintext of the relevant data and communications. To make clear that this authorization must be limited to the extent possible to the information which is actually necessary to obtain the relevant plaintext, section 2712(b) also provides that an order under that section directing the disclosure of stored recovery information shall be limited to the extent

practicable to directing the disclosure of only that stored recovery information that is necessary to allow access to the plaintext of the relevant data and communications.

The third criterion of section 2712(b) (proposed section2712(b)(3))--that the governmental entity will seek access to the plaintext within a reasonable time--is a protection designed to eliminate the possibility that governmental entities could obtain decryption keys under CESA's court-order provision and warehouse them for future use with respect to encrypted data, including data other than that for which the key was obtained. The fourth court-order criterion outlined above (proposed section2712(b)(4), that there must be no constitutionally protected expectation of privacy in the plaintext the governmental entity is seeking through use of a key or through decryption by the recovery agent, or that the privacy interest created by such expectation has been overcome) is necessary to assure that the governmental entity's use of a stored decryption key, or a recovery agent's disclosure of plaintext obtained by using a stored key, would pass constitutional muster. In other words, the government may request a key under this provision only if it may use the key to decrypt the encrypted information, without violating a person's constitutionally protected expectation of privacy. The requirement would likely be met, for example, where the governmental entity had obtained a search warrant that applies to the plaintext itself and later sought a court order for disclosure of the stored key. Under this theory the use of the key to obtain plaintext is authorized by the search warrant for plaintext.

Another feature of proposed section2712 is the notice requirement in subsection(c). Within 90days after receiving stored recovery information or decrypted data from a recovery agent, the governmental entity must notify the person, if known, who stored the recovery information that stored recovery information was disclosed or used by the recovery agent. Delay in notice is permitted for good cause.

Proposed section2712(d) provides for cost reimbursement to the recovery agent of costs that are reasonably necessary and directly incurred in providing stored recovery information or decrypting data or communications. However, this section is applicable only when the government proceeds under section 2712(b), requiring by order that a recovery agent provide stored recovery information (which must the decryption key of another person or entity) or use such information to decrypt data and communications. Because of the definition of "stored recovery information," which requires that the information disclosed or used (the decryption key) be of another, and as made clear by the exclusions of section 2711(d), no person may obtain reimbursement under this section for production of its own recovery information or for decrypting its own records, even if that person happens to be a recovery agent. In each case, no order under section 2712(b) is required.

Proposed section2712 also contains a provision aimed at assistance to foreign governments. The last paragraph of subsection(a) clarifies that a federal governmental entity--on behalf of and for the benefit of a foreign government--may require a recovery agent to disclose stored recovery information to it or another federal governmental entity, or to use stored recovery information to decrypt data or communications, pursuant to one of the mechanisms set forth in this subsection (warrant, subpoena or other process under limited circumstances, court order, or emergency determination) and pursuant to a request of the foreign government under applicable legislation, treaties, or other international agreements. For example, under this provision a foreign government could request the assistance of the federal government, which could then seek a court order to require a recovery agent to disclose stored recovery information to the federal entity or to use stored recovery information to decrypt data that would ultimately benefit the foreign government.

The foreign government's request for assistance to the federal government need not be limited to a formal request under a mutual legal assistance treaty but may be any request made by a foreign government consistent with applicable legislation, treaties, or other international agreements. For example, the United States has entered into and the Senate has ratified many mutual legal assistance treaties under which the United States gives and receives legal assistance to and from foreign sovereigns. Foreign sovereigns also may seek assistance under an older letters rogatory regime that is supported by statute (seebelow), or under other international agreements not ratified by the Senate, including executive agreements between corresponding executive authorities in the United States and a foreign state. Such executive agreements are limited in scope by Congress' grant of authority to the relevant agency. Long standing United States law governs the execution of any such request and effectively protects individual civil liberties.

Specifically, a well-established body of law and the relevant federal statute governing the execution of all foreign assistance requests bar the compelled production of anything "in violation of any legally applicable privilege." 28 U.S.C. § 1782 (emphasis added). Moreover, the mutual legal assistance treaties ratified by the Senate (which have the force of law) explicitly refer to the obligation of the United States to protect the legal and constitutional rights of United States' persons. Other international agreements similarly include such "essential interests" clauses. The United States has assisted, and will

continue to assist, other sovereigns while simultaneously guarding civil liberties.

For example, a foreign sovereign may not share the United States' essential interest in free speech under the First Amendment, and could seek to investigate constitutionally protected activity. In such a case, whether the request is made under a treaty or other international agreement, the United States asserts its essential interest in the protection of speech and refuses to provide the assistance sought.

The foreign government provision is needed because the ability of the UnitedStates to assist foreign governments in appropriate cases puts the UnitedStates in the best position to seek and obtain assistance that it will need to pursue its own critical investigations and interests. The nature of international commerce and crime is such that encrypted data containing information important to a domestic interest, such as a United States criminal prosecution, may be decrypted with a key held in another country. Obtaining that key may be critical to the United States prosecution. Further, the UnitedStates has an independent interest in assisting foreign authorities in enforcing their criminal laws and other enforcement schemes. For example, German investigators may be unable to uncover crimes by a computer hacker in Germany if that hacker has encrypted his or her communications and stored the key with a recovery agent in the United States. Assistance to foreign officials in such a case is important so that international borders do not impose insuperable burdens on criminal investigations.

While proposed section2712(a) specifies its applicability in the context of assistance to a foreign government, this provision is not intended to limit the applicability of other provisions of law upon which the federal government relies in assisting foreign governments to obtain other types of information (i.e., information other than that addressed by proposed section2712) or in providing other types of law enforcement support to foreign governments. That is, the absence of such provisions in other statutes does not imply that the UnitedStates lacks authority to use those provisions to assist foreign governments. Proposed section2712(a) merely clarifies that recovery agents may be required to disclose stored recovery information or to decrypt data or communications when a federal governmental entity seeks such information for the benefit of a foreign government. By providing explicitly for foreign government assistance, the United States ensures that it will not become a data haven for those who would circumvent their national laws by storing recovery information in the UnitedStates.

Proposed 18 U.S.C. §2713

Proposed section2713 provides limitations on the use and disclosure of recovery information obtained by a governmental entity by compulsory process and also requires destruction of such information. The protections established by this provision are broad in scope and apply to recovery information obtained from a recovery agent, as well as to recovery information obtained from other sources. Thus, proposed section2713 has broader scope than section2712, which only addresses government access to stored recovery information (which, by definition, is held by a recovery agent).

The breadth of subsection(a) is reflected in its two paragraphs. Paragraph(1) limits the use of recovery information obtained by a governmental entity from a recovery agent under proposed section2712 by requiring that an order or other authorization for access under that section must specify the categories of data and communications that may be decrypted. A further court order would be necessary for any additional uses. Paragraph(2) addresses recovery information obtained by a governmental entity through compulsory process other than under section2712. It authorizes the use of such information only in connection with the matter for which the recovery information was obtained and related matters, and only if the decryption is appropriate to the proper performance of the official functions of the governmental entity. Thus, for example, a governmental entity that uses a grand jury subpoena to obtain recovery information from a person who is not a recovery agent would be limited by subsection(a)(2) in its use of the recovery information obtained. A court of competent jurisdiction may permit further uses.

Subsection(b) of proposed section2713 imposes limitations on the disclosure and subsequent use of recovery information obtained by a governmental entity through compulsory process. This provision applies to recovery information obtained from a recovery agent under proposed section2712, and to recovery information obtained through any other compulsory process, such as a grand jury subpoena issued to a third party key-holder who is not a recovery agent. Subsection(b) allows disclosure of recovery information obtained by the governmental entity only to the extent such disclosure is in connection with the matter for which the recovery information was obtained and any related matters, and only if the disclosure is appropriate to the proper performance of the official functions of the disclosing governmental entity. Further use by the

receiving entity is governed by the limitations in subsection(a), and further disclosure by the receiving entity is also prohibited.

As in subsection (a), subsection(b) allows exceptions in accordance with an order of a court of competent jurisdiction.

Subsection(c) of proposed section 2713 concerns the destruction of recovery information. The scope of information to which it applies is as broad as that to which subsection (b) applies. Subsection (c) requires the destruction of recovery information obtained by compulsory process at a time specified by this provision and applies to a governmental entity, a recovery agent assisting a governmental entity, and any other person or entity that has received disclosure under section 2713. Any exception to these requirements must be authorized by an order of a court of competent jurisdiction.

Proposed 18 U.S.C. § 2714

Proposed section 2714 requires notice of access to recovery information held by third parties and knowingly obtained by a governmental entity by compulsory process, other than under proposed section 2712, which contain their own notice provisions. For example, under section2714 a governmental entity would be required to notify a person who had asked a friend to hold a decryption key on the former's behalf if the governmental entity had knowingly obtained the key by compulsory process, such as through a grand jury subpoena. Thus, whether a person chooses a recovery agent or a friend to hold a decryption key on his or her behalf, notice must be provided to such person of the government's access to the key. The notice must be provided within 90 days of the date on which the government obtains the key, unless the date is postponed by a court of competent jurisdiction on a showing of good cause.

Proposed 18 U.S.C. § 2715

Another amendment contained in section203 of CESA is the addition of proposed section2715 to title18, United States Code. This section would ban a cause of action against a provider of wire or electronic communications service or recovery agent and others for providing information, facilities, or assistance in accordance with the terms of a court order, emergency request, grand jury subpoena, warrant, or other process under proposed section 2711 or 2712, or for disclosing information to a governmental entity to assist it in obtaining lawful access to information protected by encryption or other security techniques or devices, unless the disclosure is otherwise prohibited by chapter 121, as amended. This provision serves as an exception to the cause of action provided for in 18U.S.C. §2707 (amended by section202 of CESA) and in effect parallels section2703(e) of current law, which places a similar ban on a cause of action against a provider of wire or electronic communication service for specified actions that accord with Chapter121 of title18, which is amended by CESA. The second part of this provision is necessary to protect those entities that assist governmental entities in obtaining access to plaintext, particularly by sharing trade secret information pursuant to proposed section 2716, from litigation based on actions they take in interests of public safety.

Proposed 18 U.S.C. § 2716

Section 203 of CESA also contains a provision designed to protect, in appropriate circumstances, against disclosure in court proceedings of government methods of access to information protected by encryption or other security techniques or devices. Proposed section2716(a) of title18, United States Code, would allow an attorney for the government to file an application requesting the court to enter an order protecting the confidentiality of a technique that provided access to such information. Section 2716(b) requires the court to enter such an order if the court finds that disclosure is likely to jeopardize an ongoing investigation, compromise the technique for the purposes of future investigations, result in physical injury to any individual, or seriously jeopardize public health and safety, or if the court finds that disclosure could reasonably be expected to affect the national security. (Such an order may also be entered by a court in order to protect trade secrets associated with access to plaintext, see below.) As the proposed statute makes clear, any such order must be consistent with constitutional requirements and limitations. Proposed section2716(b) specifically provides that a confidentiality order under this section may direct the use of special procedures, as appropriate, relating to the admissibility of evidence obtained through an access technique that the government seeks to protect from disclosure. Thus, for example, a court can devise procedures that guard a defendant's Sixth Amendment right to the confrontation of witnesses while also preserving the confidentiality of the government's access techniques.

In ruling on applications for orders under section 2712(b), the court must, of course, be careful not to require the disclosure of the confidential information that the government is attempting to protect. Therefore, using their existing authority, courts should permit the use of procedures, including in camera and sealed filings and ex parte hearings, as appropriate, with notice

to the defendant, in ruling on requests for orders under this subsection.

Section2716 applies to any civil or criminal case, whether or not the government is a party. In addition, although proposed section2716(a) authorizes that such a request be filed by an "attorney for the government" as that term is defined in the Federal Rules of Criminal Procedure (see Rule54), which generally limits the term to federal prosecutors, the court order under subsection(b) may protect the confidentiality of access techniques used by any "governmental entity." This term includes State and local governments under proposed section 2718. Thus, for example, access techniques used by a State investigator and later disclosed to federal investigators for purposes of federal prosecution will be eligible for a court order of protection.

Proposed section2716 also generally prohibits the government from disclosing trade secrets disclosed to it to assist it in obtaining access to information protected by encryption. This section provides exceptions where disclosure is to another governmental entity, is necessary to implement methods of access, is with the consent of the person or entity that owns the trade secret, or is ordered by a court of competent jurisdiction pursuant to a request of the disclosing governmental entity. In addition, in certain cases defendants in criminal cases may demand that the government disclose such trade secrets during the course of criminal proceedings. In such a case, the government must be given an opportunity to request a confidentiality order under subsection (b), as described above. If the government meets the standard described above, then the court shall enter such orders as may be necessary and appropriate to protect the trade secret, consistent with constitutional principles.

Finally, section2716 also provides that it shall not be deemed to affect the Classified Information Procedures Act.

Proposed 18 U.S.C. § 2717

The next provision in section203 of CESA is proposed section2717 of title18, United States Code, which addresses foreign intelligence information. It provides that sections2711 through 2714 shall not apply to the acquisition by the UnitedStates of foreign intelligence information as defined in section101(e) of the Foreign Intelligence Surveillance Act of 1978, or otherwise affect any lawfully authorized intelligence activity of an officer, agent, or employee of the United States, or a person acting pursuant to a contract with the United States. For example, under existing authorities, such as the Foreign Intelligence Surveillance Act, 50 U.S.C. §1801 et seq., the government is authorized to engage in electronic surveillance for the purpose of collecting foreign intelligence and foreign counterintelligence information. These authorities permit the government to direct
others to provide technical cooperation that the government deems necessary to obtain the plaintext of communications and data. Section 2717 makes clear that the government's existing authority to secure such cooperation for the purpose of collecting foreign intelligence and counterintelligence information is in no way impaired, burdened, or otherwise restricted by any provision of CESA. Appropriate restrictions on the use of information derived from and related to such intelligence and counterintelligence investigations are already implemented under existing authorities.

Section 204

Proposed 18 U.S.C. § 2718

Section204 of CESA contains definitions for Chapter121 of title18, United States Code. The definitions currently in this chapter, 18U.S.C. §2711, would be retained as new section2718(1) and (2), and many new definitions would be added. The distinction between "recovery information" and "stored recovery information" is discussed in the analysis of proposed section 2711(d).

Sections 205 and 206

Sections205 and 206 provide technical and conforming amendments.

Section 207

Section 207 authorizes appropriations for the Technical Support Center in the Federal Bureau of Investigation. This center was established pursuant to section 811(a)(1) of the Antiterrorism and Effective Death Penalty Act of 1996, and will serve as a centralized technical resource for Federal, State and local law enforcement in responding to the increasing use of encryption by criminals.

Section 301

Section301 would amend section2516(1)(c) to add felony violations of 18U.S.C. §1030, relating to computer fraud and abuse, to the list of offenses for which an order to intercept wire or oral communications may be sought. This amendment is needed because violations of section1030 are sufficiently similar to and as serious as the other specified predicate offenses, e.g., violations of 18 U.S.C. §1029. In addition, in order to obtain access to decryption keys used by persons engaged in computer intrusions--who are among those criminals most likely to use encryption to hide criminal activity--the government may find it necessary to intercept wire or oral communications.

Section 401

Section 401 creates a directive to the United States Sentencing Commission, among other things, to review the sentencing guidelines and, if appropriate, to amend them to ensure that they provide sufficiently stringent penalties to deter and punish persons who knowingly use encryption to conceal their criminal activities. This directive establishes emergency authority for such a change.

Section 402

Section 402 of CESA permits the head of a federal law enforcement agency to limit the number of sources from which it solicits bids or proposals if he or she determines that disclosure of agency needs pertaining to the procurement of sensitive equipment, goods, or services associated with obtaining plaintext might reasonably jeopardize an ongoing or future investigation or the use of such equipment, goods, or services by the agency.

Section 403

Section 403 amends section 3371 of title 5, United States Code, to provide for personnel exchange programs between industry and the federal government to further the purposes of CESA.

Section 404

Section 404 of CESA concerns severability and provides that if any provision of the Act is held invalid, the remainder of the Act shall not be affected.

Return to the CESA Page

# IATAC



August 21, 2001

To: Mr. Lawrence Downing/Ms. Zena Rogers
DTIC/OCQ

From: Abraham Usher AU
IATAC Collections Specialist

Re: ADB257057 and ADB257113

This has reference to two documents:

ADB257057 An Assessment of International Legal Issues in Information Operations

and

ADB257113 White House Document Analysis

The distribution statement on both of these documents should be changed to Distribution A – *Approved for public release.*

Thank you,

Abraham Usher

3190 Fairview Park Drive • Falls Church, VA 22042
Phone: 703.289.5454 • FAX: 703.289.5467 • STU-III: 703.289.5462
E-mail: iatac@dtic.mil • URL: http://iac.dtic.mil/iatac • SIPRNET: http://iatac.dtic.smil.mil